06277202   Supplier Number: 54409656 (THIS IS THE FULLTEXT)
Digital Stamps Promise Low-Cost Convenience.(Technology Information)
McCooey, Eileen
Windows Magazine, p27(1)
May 1, 1999
ISSN: 1060-1066
Language: English
Record Type: Fulltext
Document Type: Magazine/Journal; General Trade
Word Count: 427

TEXT:
We've all joked about printing our own money-but did you ever think about printing your own stamps?

That could become more than a pipe dream this summer if the U.S. Postal Service (USPS) approves several products now in beta tests with hundreds of businesses. When that happens, you'll be able to buy postage over the Internet and print digital stamps, called indicia, using your PC and a standard laser or ink jet printer.

That means you'll be able to buy postage around the clock without hoofing it to the local post office or footing the monthly bill for a postage meter. You should also enjoy faster, more accurate mail delivery, the USPS promises.

And to top it off, you'll save money. Many small businesses pay $50 to $75 a month for meter rental, plus fees for refilling postage. Internet postage carries only a modest service charge, typically 10% of postage costs. If you're spending $300 a month on postage-the high end of the target market-that's only $30.

Here's how it works: You download postage from a vendor such as E- Stamp or Stamps.com, two of the first entrants in the category. The USPS requires all providers to use encryption and authentication to safeguard transactions.

With software-only products like Stamps.com's, there's no hardware cost, and application software is free on the Web. But you can print postage only while connected to the Internet, so it's practical only for users with fairly low mail volume and a persistent Internet connection.

With E-Stamp's hardware and software solution, you download postage from the company's Web site and store it in an "electronic vault" connected to your PC's parallel port. That allows you to print postage as needed without reconnecting to the Internet. But it costs about $100 for the package. E-Stamp is awaiting approval on a free browser-based version that requires no hardware and no software download.

With any of these products, you print postage directly onto an envelope, label or document from within a standard Windows application that generates a name and address, such as a word processor or database program. The indicium consists of readable text and a bar code that includes a digital signature and the address, postage rate and *mailing* *date*. To prevent *fraud*, each *indicium* is unique and can't be photocopied, and postage can be printed only with a valid mailing address.

While the first offerings are aimed at small businesses and consumers, variations for high-volume corporate customers with mainframe or client-server environments are expected to follow.

PUB-NO: EP000856816A2
DOCUMENT-IDENTIFIER: EP 856816 A2
TITLE: Method and apparatus for printing and prevention of copying of postage indicia
PUBN-DATE: August 5, 1998
INVENTOR-INFORMATION:
NAME   COUNTRY
HERBERT, RAYMOND JOHN   GB
INT-CL (IPC):   G07B017/00
EUR-CL (EPC):   G07B017/00

ABSTRACT:

CHG DATE=19990617 STATUS=O> Postage indicia (12) are printed on mail items (10) using an ink having a characteristic such that the ink is rendered invisible when subjected to light or light and heat of sufficient intensity. When an attempt is made to copy the imprint of a postage indicia (12) on a mail item for which proper accounting has been effected the imprint is subjected to a burst of light or light and heat and the ink becomes invisible and prevents copying of the imprint. The imprint of the postage indicium may overly and obscure a void mark (14) which becomes visible and is copied in the event of attempting to copy the original authentic postage indicium (12).
<IMAGE>

US-PAT-NO: 5513563
DOCUMENT-IDENTIFIER: US 5513563 A
TITLE: Indicia security via variable dot size
DATE-ISSUED: May 7, 1996
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Berson; William	Weston	CT	N/A	N/A

US-CL-CURRENT: 101/91, 235/101 , 347/15 , 382/299 , 400/124.3 , 05/408

ABSTRACT: A system is disclosed that makes it more difficult to print fraudulent indicia. Security is achieved by varying the dot size of pixels in the printed image according to a predetermined arrangement.
5 Claims,   5 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 3

---------- KWIC ---------

Brief Summary Text - BSTX (8): This invention overcomes the disadvantages of the prior art by providing a system that makes it more difficult to print fraudulent indicia. The apparatus of this invention provides a device for verifiable security in a postage meter or other device using dot matrix or bit-addressable printing. Security is achieved by varying the dot size of pixels in the printed image according to a predetermined arrangement. The dot size variation is used to encode the meter serial number, ascending and descending funds registers, mail piece identifier date, time and origin of mail piece and other data which may be used for indicia variation and to prevent fraud.

US-PAT-NO: 5688056
DOCUMENT-IDENTIFIER: US 5688056 A
TITLE: Method for controlling a printer in order to obtain postages
DATE-ISSUED: November 18, 1997
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Peyret; Patrice	Fuveau	N/A	N/A	FR

US-CL-CURRENT: 400/61, 235/382 , 400/103

ABSTRACT: Methods enabling the use of an office printer connected to a microcomputer in order to print legitimate postal marks. It uses a cartridge of special fonts in which there are stored the franking marks according to the standards laid down for the printer. A known security component is provided, on the one hand to protect access to the memory contained in the cartridge and, on the other hand, to perform the computation, for each printing of a franking mark, of a security mark that contains encrypted information elements that are readable by the postal authority, enabling the franking mark to be authenticated. It provides for the elimination of specific franking machines and limits the handling operations to the handling of a small-sized cartridge.
19 Claims,   6 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 2

--------- KWIC ---------

Detailed Description Text - DETX (6): The security mark will therefore comprise, in an encrypted form, all the particulars needed for identifying the cartridge and hence its possessor, i.e. essentially an identification number. It could furthermore comprise particulars pertaining to date and time enabling the subsequently used checking devices to compare the date and the time that may be printed on the franking mark so as to detect any attempts at fraud in a relatively simple way. These particulars could be obtained in the cartridge in this case by means of a clock saved by a long-life battery, according to a known method. This clock could then be used to restrict the duration of use of the cartridge, for example in the case of a fixed-price and fixed-period franking contract or, to oblige the user of the cartridge to have it checked at regular intervals. The latter point will be especially useful for the more frequent case where the cartridge has a counter that increments the fee units as and when it is used, as this counter will have to be read by the Post Office so that the user can be invoiced.

US-PAT-NO: 6005945
DOCUMENT-IDENTIFIER: US 6005945 A
TITLE: System and method for dispensing postage based on telephonic or web milli-transactions
DATE-ISSUED: December 21, 1999
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE
Whitehouse; Harry T.	Portola Valley	CA	N/A

US-CL-CURRENT: 380/51

ABSTRACT: A system for electronic distribution of postage includes at least one secure central computer for generating postal indicia in response to postage requests submitted by end user computers, and at least one postal authority computer system for processing the postal indicia on mail pieces. A key aspect of the system is that all secure processing required for generating postal indicia is performed at secure central computers, not at end user computers, thereby removing the need for specialized secure computational equipment at end user sites. A secure central computer includes a database of information concerning user accounts of users authorized to request postal indicia from the secure central computer. A request validation procedure authenticates received postage requests with respect to the user account information in the database. A postal indicia creation procedure, applies a secret encryption key to information in each authenticated postage request so as to generate a digital signature and combines the information in each authenticated postage request with the corresponding generated digital signature so as to generate a digital postage indicium in accordance with a predefined postage indicium data format. A communication procedure securely transmits the generated digital postage indicium to the requesting end user computer. Each end user computer typically includes a communication procedure for sending postage requests to a secure central computer at which a user account has been established, and for receiving a corresponding digital postage indicium. A postage indicium printing procedure prints a postage indicium in accordance with the received digital postage indicium.
12 Claims,   9 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 8

---------- KWIC ---------

Detailed Description Text - DETX (153): The meter information database 270 includes a small subset of the information in the customer database 172 in the secure central computers 102, and in particular just the information needed for verifying postal indicia. Updated data concerning all licensed "meters" (i.e., end user computers) is preferably downloaded from the secure central computers periodically, such as once a day. In addition, to the information retrieved from the secure central computers, the meter information database preferably will also include a compact serial number usage bit map, or equivalent mechanism, for keeping track of all serial numbers used by each licensed meter in the last week or so. The serial number usage bit map is updated every

time a mail piece postage indicium is authenticated, and provides a quick mechanism for detecting duplicate postal indicia, which would expected to be the most common form of attempted fraud. As a result, the transaction database 272 is accessed only for (A) storing records of authenticated and rejected mail pieces, and (B) postal indicia error and fraud investigations. The size of the bit map is preferably variable so as to accommodate high volume accounts, ranging from a couple of hundred bits for low volume accounts to perhaps a 10K bits or more for the most active accounts. A preferred format of the serial number usage bit map within the database record for each licensed meter account is:

US-PAT-NO: 6249777
DOCUMENT-IDENTIFIER: US 6249777 B1
TITLE: System and method for remote postage metering
DATE-ISSUED: June 19, 2001
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kara; Salim G.	Markham	N/A	N/A	CA
Pagel; Martin J.	Kirkland	WA	N/A	N/A

US-CL-CURRENT: 705/404, 705/401 , 705/60 , 705/62

ABSTRACT: A system and method for remote postage metering of postage indicia, including demanding a desired postage amount and subsequently printing the postage indicia onto a piece of mail. A user inputs certain necessary information, as well as additional desired information, into a local processor-based system. The local system then assembles a postage demand in suitable format and transmits the same to a remote postage metering device. The remote postage metering device then verifies the demand for authority to demand and valid funding. Upon verification, the remote postage meter assembles a data packet representing an authorized postage indicia. The data packet is transmitted to the local system for printing. Printing of the postage indicia may be unaccompanied, or may include additional information. Such additional information may include destination and return address, machine readable routing or identification information, or a complete document to be posted.

67 Claims,   4 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 3

---------- KWIC ---------

Detailed Description Text - DETX (42): Step 215 involves integrating the data packet with any other data to be printed on the postal item. A substep of decrypting the received data packet, utilizing a private key of the PPK held at the demanding system, is utilized if encryption is desired. Decryption of the data packet near the time of printing the postage indicia is advantageous in preventing postal fraud accomplished by multiple uses of a single data packet. However, decryption may be accomplished at any time prior to printing the postage indicia. Of course, step 215 may be omitted if integration with other data or encryption is not desired.

Detailed Description Text - DETX (48): Furthermore, including a unique transaction number within the printed postage indicia aids in the detection of postage fraud. This unique transaction is machine readable, and upon two occurrences of the same transaction number, postage fraud is indicated. Moreover, a transaction number may be generated so as to indicate the remote postage metering device that originally distributed the postage credit. With this information, determination of the demanding PC is a simple process of reviewing transaction logs at the remote metering device.

PGPUB-DOCUMENT-NUMBER: 20020035547
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020035547 A1
TITLE: Franking method and apparatus
PUBLICATION-DATE: March 21, 2002
INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Bleumer, Gerrit	Velten	DE		

US-CL-CURRENT: 705/62, 705/408

ABSTRACT: In a method and system and franking apparatus for franking postal matter and for inspection of the franking, postage fees are stored and debited in electronic form, and a fee stamp and a machine-readable date stamp containing encrypted data are applied to the postal matter. In order to satisfy high security demands to be met at a low cost, and to allow realization on a standard computer with a printer without additional hardware, an individual date stamp, distinguishable from the date stamps generated for other pieces of mail is generated for each piece of mail and is applied to the piece of mail. An inspection for multiple employment of postage fees and/or date stamps ensues on the basis of the date stamp. This inspection includes comparing a date stamp to be inspected to previously used date stamps stored in a data bank. Defrauders thus can be identified who, without paying, attempt to generate frankings or to multiply employ frankings, for example by copying.

---------- KWIC ---------

Detail Description Paragraph - DETX (6): [0031] At any point in time, the mail-carrying system should only carry as much mail as is covered by paid fees. As a sub-criterion, double employment of postage fees should be prevented: after a user has downloaded postage fees amounting to a value of x, the user should be able to print out a maximum of fee stamps whose total value does not exceed the value x. In open franking systems, the recipient address and a time mark are usually already contained in the date stamp, so that a renewed use of a franking that has already been employed is largely precluded, even without further cryptographic security measures. In closed franking systems, wherein the franking process is separate from the address in process, so that the recipient address is usually not contained in the date stamp, copies of frankings nonetheless can be detected by, as in the inventive system, comparing frankings, i.e. the date stamp of a franking, to frankings that have already been used and are stored in a data bank upon being inspected. If a date stamp is detected for a second time, then the postal matter franked therewith either can be charged a punitive postage and sent back to the sender, or can be precluded from mail-carrying. As a further protective measure to prevent copying of frankings, red fluorescent ink can be employed for the fee and/or date stamp, this being very difficult to reproduce with conventional copiers. In order to identify a user who illegally employs a postage fee unit multiple times for franking, the date stamp can contain data about this user in non-manipulatable form, for example the number of the user's postage fee account or a specific user code.

NAME	CITY	STATE	COUNTRY	RULE-47
Heiden, Gary M.	Shelton	CT	US	
Heiden, Richard W.	Huntington	CT	US	
Li, Chunhua	North Haven	CT	US	

ABSTRACT: A system for generating digital postage stamps wherein a PC requests digital postage stamps from a data center. The data center generates a digital book of postage stamps, which the PC downloads to its hard drive. The digital book of postage stamps includes a read-only software module that prints each digital postage stamp using stamp related information contained within the software module. The software module on the PC verifies that the signature of the PC is identical to the PC signature that was stored in the software module when the software module was configured at the data center. If verified, the software module generates the digital postage stamp and then initiates printing on a printer coupled to the PC. The software module renders the data associated with the digital postage stamp being printed unusable for subsequent generations of digital postage stamps.

---------- KWIC ---------

Detail Description Paragraph - DETX (17): [0042] One way of detecting such duplication fraud is to audit the information contained within the digital postage stamp to verify that the stamp is being audited for only one time. Such an audit can be achieved by maintaining a database of all digital postage stamps audited for a period, such as a month. This audit process can be made more reliable by placing a time limit that the digital postage stamps may be printed. The time limit may be in the form of a date range, for example two weeks from the time of purchase, so that the period for maintaining the database is reliably reasonable. Another method for auditing for duplicates is to maintain a list of generated digital postage stamps by server. When a digital postage stamp is audited, the audit process compares the audited stamp to the list of stamps to verify that the stamp has not been audited more than once. Preferably, the comparison is limited to the sequential number of the digital postage stamp by server.

1

US-PAT-NO: 6438530
DOCUMENT-IDENTIFIER: US 6438530 B1
TITLE: Software based stamp dispenser
DATE-ISSUED: August 20, 2002
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Heiden; Gary M.	Shelton	CT	N/A	N/A
Heiden; Richard W.	Huntington	CT	N/A	N/A
Li; Chunhua	North Haven	CT	N/A	N/A

US-CL-CURRENT: 705/401, 705/408 , 705/410 , 705/60

ABSTRACT: A method for generating digital postage stamps wherein a data center receives a request from a PC for a selected number of digital postage stamps, concludes a payment transaction for the selected number of digital postage stamps, generates a digital book of postage stamps, which the PC downloads to its hard drive. The digital book of postage stamps includes a read-only software module that prints each digital postage stamp using stamp related information contained within the software module. The stamp related information includes stamp information, which is required for each postage stamp, user information, which identifies the requester and the PC, data center server information, which is unique to each digital postage stamp and a digital signature of at least some of the user, stamp and/or server information. Before printing a digital postage stamp, the software module on the PC verifies that the signature of the PC is identical to the PC signature that was stored in the software module when the software module was configured at the data center server. If verified, the software module generates the digital postage stamp using the stamp, user and server data associated with the digital postage stamp and then initiates the printing of the digital postage stamp on a printer coupled to the PC. The software module renders the stamp, user and server data associated with the digital postage stamp being printed unusable for subsequent generations of digital postage stamps.

22 Claims,   7 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 6

---------- KWIC ---------

Detailed Description Text - DETX (8): At step 410, if the signatures are not identical, then at step 420, the software module displays an appropriate message to the user and does not print the requested digital postage stamp. If the signatures are identical, then at step 430, the software module generates the digital postage stamp using the stamp data, user data and server data that stored within the software module. A more complete description of the stamp data, user data and server data is provided below. At step 440, the software module initiates the printing of the digital postage stamp on a printer coupled to the PC. At step 450, the software module prevents duplicate printing of a digital postage stamp by making the data used in generating the digital postage stamps that is being printed, i,e., the stamp data, user data and server data, unusable for subsequent generations of digital postage stamps. At step 460, the software module

determines if all postage stamps in the digital postage stamps have been printed. If all stamps have been printed, then at step 470, the software module notifies the user and uninstalls itself from the PC hard drive. If all stamps in the book have not been printed, the method returns to step 400 to enable generation of another digital postage stamp. Referring now to FIG. 5, a block diagram representative of a digital book of postage stamps is shown. The digital book of postage stamps comprises a software module, generally designated 500, which includes application software 510 that runs in only one PC to generate and print digital postage stamps using digital postage stamp data files stored within software module 500. For each digital postage stamp in the digital book of postage stamps, a digital postage stamp data file includes: stamp data 520, such as origin zip code of the PC, denomination of the digital postage stamp and date of request; user data 530, such as user identification number and PC signature information; server data 540, such as identification of the server that generated software module 500, status information of the server and a number corresponding to this postage stamp's sequential number of digital postage stamps generated by the server; and a digital signature of the postage stamp 550. The digital signature of the postage stamp is generated at the data center using a cryptographic key to sign at least some of the postage stamp data 520-550. Preferably a private key of a public key pair, for example as used in the RSA public key algorithm. Finally, software module includes a number 560 that represents the number of unused stamps remaining in the book of stamps. This number 560 is decremented by software module 500 each time a stamp is printed by the software module.

Detailed Description Text - DETX (16): One way of detecting such duplication fraud is to audit the information contained within the digital postage stamp to verify that the stamp is being audited for only one time. Such an audit can be achieved by maintaining a database of all digital postage stamps audited for a period, such as a month. This audit process can be made more reliable by placing a time limit that the digital postage stamps may be printed. The time limit may be in the form of a date range, for example two weeks from the time of purchase, so that the period for maintaining the database is reliably reasonable. Another method for auditing for duplicates is to maintain a list of generated digital postage stamps by server. When a digital postage stamp is audited, the audit process compares the audited stamp to the list of stamps to verify that the stamp has not been audited more than once. Preferably, the comparison is limited to the sequential number of the digital postage stamp by server.

File   2:INSPEC 1969-2004/Dec W2 (c) 2004 Institution of Electrical Engineers
File   9:Business & Industry(R) Jul/1994-2004/Dec 27 (c) 2004 The Gale Group
File   15:ABI/Inform(R) 1971-2004/Dec 24 (c) 2004 ProQuest Info&Learning
File   16:Gale Group PROMT(R) 1990-2004/Dec 28 (c) 2004 The Gale Group
File   20:Dialog Global Reporter 1997-2004/Dec 28 (c) 2004 The Dialog Corp.
File   35:Dissertation Abs Online 1861-2004/Dec (c) 2004 ProQuest Info&Learning
File   65:Inside Conferences 1993-2004/Dec W3 (c) 2004 BLDSC all rts. reserv.
File   99:Wilson Appl. Sci & Tech Abs 1983-2004/Nov (c) 2004 The HW Wilson Co.
File   148:Gale Group Trade & Industry DB 1976-2004/Dec 28 (c)2004 The Gale Group
File   160:Gale Group PROMT(R) 1972-1989 (c) 1999 The Gale Group
File   233:Internet & Personal Comp. Abs. 1981-2003/Sep (c) 2003 EBSCO Pub.
File   256:TecInfoSource 82-2004/Dec (c) 2004 Info.Sources Inc
File   275:Gale Group Computer DB(TM) 1983-2004/Dec 28 (c) 2004 The Gale Group
File   347:JAPIO Nov 1976-2004/Aug(Updated 041203) (c) 2004 JPO & JAPIO
File   348:EUROPEAN PATENTS 1978-2004/Dec W02 (c) 2004 European Patent Office
File   349:PCT FULLTEXT 1979-2002/UB=20041223,UT=20041216 (c) 2004 WIPO/Univentio
File   474:New York Times Abs 1969-2004/Dec 27 (c) 2004 The New York Times
File   475:Wall Street Journal Abs 1973-2004/Dec 27 (c) 2004 The New York Times
File   476:Financial Times Fulltext 1982-2004/Dec 28 (c) 2004 Financial Times Ltd
File   583:Gale Group Globalbase(TM) 1986-2002/Dec 13 (c) 2002 The Gale Group
File   610:Business Wire 1999-2004/Dec 27 (c) 2004 Business Wire.
File   613:PR Newswire 1999-2004/Dec 27 (c) 2004 PR Newswire Association Inc
File   621:Gale Group New Prod.Annou.(R) 1985-2004/Dec 28 (c) 2004 The Gale Group
File   624:McGraw-Hill Publications 1985-2004/Dec 27 (c) 2004 McGraw-Hill Co. Inc
File   634:San Jose Mercury Jun 1985-2004/Dec 24 (c) 2004 San Jose Mercury News
File   636:Gale Group Newsletter DB(TM) 1987-2004/Dec 28 (c) 2004 The Gale Group
File   810:Business Wire 1986-1999/Feb 28 (c) 1999 Business Wire
File   813:PR Newswire 1987-1999/Apr 30 (c) 1999 PR Newswire Association Inc

Set	Items	Description
S1	224274	(POSTAGE OR FRANK???? OR MAIL??? OR SHIPPING) (5N) (INDICIA OR INDICIUM OR MARK??? OR STAMP??? OR IMPRESSION OR IMPRINT)
S2	4789	(FAIL OR FAILED OR FAILURE) (3N) (VERIFY OR VERIFICATION OR VERIFIED OR VERIFYING OR AUTHENTICAT????)
S3	610	S1 (5N) (S2 OR COPY OR COPIED OR COPYING OR DUPLICAT???? OR FRAUD OR FRAUDULENT OR UNAUTHORIZED OR UNVERIFIED OR UNAUTHENTICATED OR TAMPER OR TAMPERING)
S4	237936	(UNIQUE OR RANDOM OR ID OR IDENTIFICATION OR PIECE OR ITEM) (5N) (COUNT OR NUMBER OR SERIAL)
S5	4344	S1 (5N) (S4 OR DATE OR TIME OR PERIOD OR INTERVAL)
S6	23	S3 (S) S5
S7	18	RD S6 (unique items) [Scanned ti,pd,kwic all]